CLAIMS:

1. (Previously presented) A method, in a data processing system, for handling personally identifiable information, said method comprising:

providing, in a computer, a first set of object classes, of an object model in an object oriented programming language, representing active entities in an information-handling process;

providing, in said computer, a second object class, of the object model, representing personally identifiable information and associated rules in said information-handling process; and

processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said first set of object classes and said second object class of the object model, so as to enforce a privacy policy, wherein

said rules define if and how said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.

2. (Previously presented) The method of claim 1, wherein said first set of object classes include one or more object classes representing parties, selected from the group consisting of:

a data user object class,

a data subject object class,

a guardian object class, and

a privacy authority object class.

3. (Previously presented) The method of claim 1, wherein said second object class, having said rules associated with said data, represents a filled paper form, including both collected data, collected from the active entity and including the personally identifiable information, and rules regarding said collected data specifying if and how the collected data is provided to the second data user, wherein the second data user sends an empty form including a policy to the first data user requesting the personally identifiable information, and wherein the first data user checks the

policy included with the empty form to determine if disclosure of the personally identifiable information is permitted based on the policy included with the empty form and the rules regarding the collected data.

4-18. (Canceled)

19. (Previously presented) The method of claim 1, further comprising:

transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

20-22. (Canceled)

23. (Previously presented) The method of claim 1, wherein said privacy policy is associated with the personally identifiable information and defined by said rules, and is enforced against one or more active entities represented by said first set of object classes, and wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity.

24. (Previously presented) The method of claim 1, wherein:

a first active entity represented by a first object class in said first set of object classes is said first data user that previously requested said personally identifiable information from said data subject that is a second active entity represented by a second object class in said first set of object classes, and

a third active entity represented by a third object class in said first set of object classes is said second data user that requests said personally identifiable information from said first data user.

25. (Previously presented) The method of claim 19, wherein said transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing

said personally identifiable information to the second data user comprises removing information that relates the personally identifiable information to the data subject in a reversible manner.

26. (Previously presented) The method of claim 1, further comprising:

transforming, based on said rules, said personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data user, wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner.

27. (Currently amended) ~~An information handling system~~ A computer system for handling personally identifiable information, said computer system comprising:

~~a processor; and~~

~~a memory coupled to the processor, wherein the memory comprises instructions which, when executed by the processor, cause the processor to:~~ a central processing unit (CPU), a computer-readable memory, and a computer readable, tangible storage device;

program instructions, stored on the storage device for execution by the CPU via the memory, to provide a first set of object classes, of an object model in an object oriented programming language, representing active entities in an information-handling process;

program instructions, stored on the storage device for execution by the CPU via the memory, to provide a second object class, of the object model, representing personally identifiable information and associated rules in said information-handling process; and

program instructions, stored on the storage device for execution by the CPU via the memory, to process transactions involving said personally identifiable information, using said first set of object classes and said second object class of the object model, so as to enforce a privacy policy, wherein said rules define if and how said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.

28. (Currently amended) The computer system of claim 27, ~~wherein the instructions~~ further ~~cause the processor~~ comprising:

program instructions, stored on the storage device for execution by the CPU via the memory, to transform, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

29. (Currently amended) The computer system of claim 27, wherein said privacy policy is associated with the personally identifiable information and defined by said rules, and is enforced against one or more active entities represented by said first set of object classes, and wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity.

30. (Currently amended) The computer system of claim 27, wherein:

a first active entity represented by a first object class in said first set of object classes is said first data user that previously requested said personally identifiable information from said data subject that is a second active entity represented by a second object class in said first set of object classes, and

a third active entity represented by a third object class in said first set of object classes is said second data user that requests said personally identifiable information from said first data user.

31. (Currently amended) The computer system of claim 28, wherein:

~~said transforming~~ the program instructions to transform, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user comprises removing information that relates the personally identifiable information to the data subject in a reversible manner.

32. (Currently amended) The computer system of claim 27, ~~wherein the instructions~~ further ~~cause the processor~~ comprising:

program instructions, stored on the storage device for execution by the CPU via the memory, to transform, based on said rules, said personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data user, wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner.

33. (Currently amended) ~~A computer program product comprising a computer-usable storage medium having computer-executable instructions stored thereon for handling personally identifiable information, wherein said computer-executable instructions, when executed by a computing device, cause the computing device to~~ A computer program product comprising a computer-readable, tangible storage device and computer-readable program instructions stored on the computer-readable, tangible storage device to handle personally identifiable information, the computer-readable program instructions, when executed by a central processing unit (CPU):

provide a first set of object classes, of an object model in an object oriented programming language, representing active entities in an information-handling process;

provide a second object class, of the object model, representing personally identifiable information and associated rules in said information-handling process; and

process transactions involving said personally identifiable information, using said first set of object classes and said second object class of the object model, so as to enforce a privacy policy, wherein said rules define if and how said personally identifiable information is provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.

34. (Currently amended) The computer program product of claim 33, ~~wherein the instructions further cause the processor to~~ further comprising computer-readable program instructions which are stored on the computer-readable, tangible storage device and when executed by the CPU:

transform, based on said rules, said personally identifiable information into a

depersonalized format prior to providing said personally identifiable information to the second data user.

35. (Previously presented) The computer program product of claim 33, wherein said privacy policy is associated with the personally identifiable information and defined by said rules, and is enforced against one or more active entities represented by said first set of object classes, and wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity.

36. (Previously presented) The computer program product of claim 33, wherein:

a first active entity represented by a first object class in said first set of object classes is said first data user that previously requested said personally identifiable information from said data subject that is a second active entity represented by a second object class in said first set of object classes, and

a third active entity represented by a third object class in said first set of object classes is said second data user that requests said personally identifiable information from said first data user.

37. (Currently amended) The computer program product of claim 34, wherein ~~said transforming~~ the computer-readable program instructions to transform, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user comprises removing information that relates the personally identifiable information to the data subject in a reversible manner.

38. (Currently amended) The computer program product of claim 33, ~~wherein the instructions further cause the processor to~~ further comprising computer-readable program instructions which are stored on the computer-readable, tangible storage device and when executed by the CPU:

transform, based on said rules, said personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data

user, wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner.

39. (Currently amended) The computer system of claim 31, wherein:

the ~~transforming is performed by~~ program instructions to transform comprise invoking a Depersonalize method contained in a data user object class in the first set of object classes, and wherein the Depersonalize method operates to strip off enough information elements in the personally identifiable information to prevent linking the personally identifiable information to an individual data subject object.

40. (Currently amended) The computer system of claim 32, wherein:

the ~~transforming is performed by~~ program instructions to transform comprise invoking an Anonymize method contained in a data user object class in the first set of object classes, and wherein the Anonymize method operates to strip off all information elements in the personally identifiable information that link the personally identifiable information to an individual data subject object.